Blockchain Applied to Security in Industrial Internet of Things Devices

Paulo Henrique Mariano[a], Charles Tim Batista Garrocho[b], Carlos Frederico Cavalcanti[c] and Ricardo Augusto Rabelo Oliveira[d]

Computing Department (DECOM), Federal University of Ouro Preto (UFOP), Ouro Preto 35400-000, Brazil

Keywords: Blockchain, Industry 4.0, Industrial Internet of Things, Cybersecurity.

Abstract: The combination of blockchain and the Industrial Internet of Things brings a set of possibilities in Industry 4.0, allowing the implementation of robust and intelligent cyber-physical systems. An important issue is that the system must be secure, ensuring that data are transmitted reliably, at a time that meets temporal requirements and is immune to cyberattacks. Despite the efficiency and innovation provided by Industrial Internet of Things devices, they face significant cybersecurity challenges due to their limited capacity and exposure to risks. This article addresses aspects of data security in industrial applications in the context of Industry 4.0, understanding that the blockchain is a robust and affordable solution that offers immutability and data decentralization. Through a literature review, we examine the benefits and challenges of blockchain adoption, such as its scalability and integration with limited devices. The study points to the need for future research into the practical application of blockchain in Industrial Internet of Things environments, evaluating its effectiveness against complex cyberattacks.

1 INTRODUCTION

Industry 4.0 has attracted the attention of companies from various sectors. In this new era of the industrial revolution, the integration between physical and digital systems is the central nerve that opens the doors to gains and possibilities. Industrial Internet of Things (IIoT) devices have been widely used for this integration. Through an IIoT device, we can collect real-time data from machines, and this data can be used to increase worker safety, optimize production, reduce waste, etc.

Despite the various benefits of these devices, we have challenges in adopting this technology, and among them is cybersecurity (Fernández-Caramés and Fraga-Lamas, 2019). Because they are generally small and have limited processing power and memory, many do not have or allow the implementation of advanced security features (Márcio et al., 2021). Another point of attention is that they can be exposed to physical risks or unauthorized human interference. Maintenance and firmware updates are another security bottleneck, if placed in hard-to-reach or risky locations (heights, unhealthy environments, etc.), maintenance routines and firmware updates become compromised.

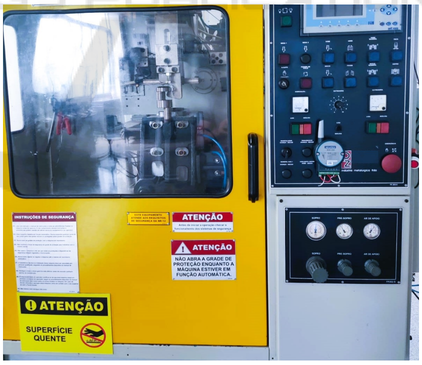


Figure 1: An industrial retrofit: machine with an adapted IIoT device. A common case in the Industrial environment.

1.1 Contribution

In this work, we present an overview of the Blockchain Applied to Security in Industrial Internet of Things Devices. Our contribution points to the need for future research on the practical application of blockchain in Industrial Internet of Things environments, evaluating its effectiveness against complex cyberattacks.

[a] https://orcid.org/0009-0001-0505-3879
[b] https://orcid.org/0000-0001-8245-306X
[c] https://orcid.org/0000-0002-8522-6345
[d] https://orcid.org/0000-0001-5167-1523

Mariano, P., Garrocho, C., Cavalcanti, C. and Oliveira, R.
Blockchain Applied to Security in Industrial Internet of Things Devices.
DOI: 10.5220/0012692500003690

In *Proceedings of the 26th International Conference on Enterprise Information Systems (ICEIS 2024) - Volume 1*, pages 345-353
ISBN: 978-989-758-692-7; ISSN: 2184-4992

These vulnerabilities particularly compromise the security of the data trafficked, attacks such as Man-in-the-Middle (MITM), Denial of Service (DoS), and credential theft, for example, can have a catastrophic impact on the company. Such challenges have inhibited the adoption of these devices, causing delays in technological and productivity advancements relevant to society. Companies that have adopted this technology are exposed to the risks of cyber threats, so common in current times.

2 RELATED WORK

In this section, we have conducted a brief review of the technologies involved in the study. Here, we also present a literature review of works published in prestigious journals, compiling these studies and highlighting the main aspects explored by the authors.

2.1 Industry 4.0

Industry 4.0 is the term used to refer to the fourth industrial revolution. It began to spread in the 2000s and involves the massive adoption of software applied to industrial processes for automation and intelligence. The union of software with machines produces what we call cyber-physical systems. The real-time sharing of data produced by machines and sensors with systems opens the door to a series of other technologies such as artificial intelligence, big data, advanced robotics, cloud computing, etc. The goal of integration and all the involved technologies is to improve efficiency, productivity, competitiveness, and innovation.

2.2 Industrial Internet of Things - IIoT

IIoT is an extended concept of IoT (Internet of Things) applied in the industrial context. IoT is the means of connecting physical devices and systems through networked devices. It plays a central role in the fourth industrial revolution (Industry 4.0) as it enables the sharing of data between cyber-physical systems, facilitating connections between various systems and machines.

2.3 Blockchain

Blockchain is a distributed ledger technology, which functions like a 'ledger book' that records transactions on this network, with each node (participating computer) validating the block of trafficked data and storing it. To validate the data, consensus algorithms known as Proof of Work and Proof of Stake are used. Another concept is “Smart Contracts”, which are algorithms that execute an action on the blockchain whenever a predefined action is performed, all the 'nodes' of the network receive this algorithm and execute it according to the defined logic.

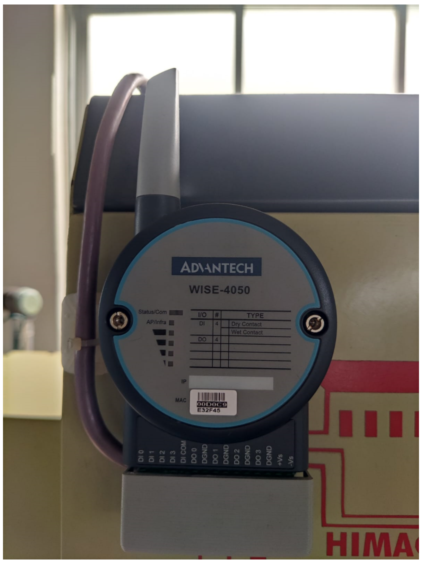


Figure 2: IIoT device.

2.4 Programmable Logic Controller – PLC

PLC is a type of digital computer that is used in industrial automation to control manufacturing processes. It is designed to operate in industrial environments to enable the control of machinery and processes. A PLC consists of a Central Processing Unit (CPU), memory, input/output (I/O) ports, power supply, and communication interfaces. The CPU runs a program stored in memory that instructs the PLC to perform certain actions based on input signals and then sends output signals to control equipment or processes. PLCs are programmed using specific languages such as Ladder Diagrams, Instruction Lists (IL), Function Block Diagram (FBD), Structured Text (ST), and Sequential Function Charts (SFC). In our architecture, it simulates data coming from an industrial machine and acts as a data publisher.

2.5 Message Queuing Telemetry Transport – MQTT

MQTT is a lightweight, publish-subscribe-based messaging protocol built on the TCP/IP model, designed for network connections with limited bandwidth or unreliable connectivity. It is used in IoT applications and Machine-to-Machine (M2M) communication because it is lightweight and requires minimal computational resources (Akshatha and Dilip Kumar, 2023). MQTT uses a small header (2 bytes) and is efficient in terms of both bandwidth usage and power consumption. MQTT follows a publish-subscribe model.

Clients connect to a central server called a broker. Clients can be publishers, subscribers, or both. Publishers send messages to the broker, associating them with a ”topic.” Subscribers subscribe to topics of interest and receive messages from the broker when they are published on those topics. Topics are strings that the broker uses to filter messages for each subscribing client. For security, MQTT supports SSL/TLS for encrypted communication. It can include username and password authentication and supports advanced security mechanisms like TLS for mutual security authentication.

An important aspect of publishing a topic is defining the Quality of Service (QoS). It refers to the assurance of a certain level of data transmission quality, especially in networks that may experience congestion or poor connectivity. QoS is essential to ensure that critical data is transmitted with the required reliability and priority, but each QoS level impacts transmission speed and computational resource consumption. These levels are:

QoS 0 (At most once): The message is sent at most once, and no acknowledgment is expected or sent. It is the fastest mode but does not provide a delivery guarantee.

QoS 1 (At least once): The message is delivered at least once. The receiver sends an ACK (acknowledgment), and the sender resends the message until it receives the ACK.

QoS 2 (Exactly once): Ensures that the message is received exactly once by the receiver. It is the most secure level but also the slowest due to its four-step handshake process.

In our architecture, we use the MQTT protocol to create a data distribution and collection point, which is used in all architecture components. Broker MQTT:

The MQTT broker serves as a hub for publishing and distributing messages from the PLC and collected by the nodes of the blockchain.

2.6 Literature Review

The *Blockchain* can enhance the automation and security of industrial processes and M2M communication. In this context, a study was conducted to identify blockchain-based research in Industry 4.0. Following the protocol of Kitchenham (2004) (Kitchenham, 2004), searches were carried out from August to December 2023 in the digital libraries: ACM, Google Scholar, IEEE Xplore, and ScienceDirect (Elsevier). For the research, the following search string was used: *blockchain and Industry 4.0; Cybersecurity IoT; Blockchain and IoT*. Regarding the selection criteria for the articles found, only those that provided full text in English were selected.

The article (Angle et al., 2019) reports that with increasing Internet connectivity and the use of reconfigurable devices, industrial control systems are more vulnerable to cyberattacks. These attacks can cause physical damage to equipment and infrastructure, and even threaten human lives. The paper explores real cyberattacks that caused physical damage, such as the Aurora Vulnerability, attacks on Ukraine’s electric power system, the explosion of a pipeline in Turkey, and the Stuxnet attack on Iran’s uranium enrichment program (Langner, 2011). It analyzes how these attacks were carried out and their consequences, highlighting the possibility of simultaneous attacks on multiple devices, which can cause extensive and difficult-to-recover damage. The study includes a case study of a small-scale cyberattack on a Variable Frequency Drive (VFD), demonstrating how malicious software can cause real physical damage. The document concludes that industrial control systems, especially those with energy storage components or physical system control, are susceptible to a variety of physical damages if they are poorly configured or maliciously attacked. It is crucial to investigate and mitigate these threats to ensure the safety and integrity of these systems.

In the article (Fernández-Caramés and Fraga-Lamas, 2019), the authors discuss how blockchain can be applied in Industry 4.0 smart factories to enhance cybersecurity, data immutability, decentralization, and automation through smart contracts. The benefits of blockchain, such as enhanced security, trust, immutability, disintermediation, decentralization, and a higher degree of automation, are highlighted. It also addresses significant challenges that blockchain implementation faces in Industry 4.0, including issues of scalability, cryptographic systems for resource-constrained devices, consensus algorithm selection, privacy and security, energy efficiency, latency, and necessary infrastructure. It studies specific industrial applications where the blockchain can be beneficial, including inventory management, traceability, and monitoring systems. The article concludes that Industry 4.0 is changing the way factories operate and that blockchain can significantly improve Industry 4.0 technologies, bringing substantial benefits in terms of security and efficiency.

In the article (Alajlan et al., 2023), the authors review various articles on the topic, addressing vulnerabilities of IoT devices caused by firmware obsolescence, physical threats, user authentication, data exposure, and low computational and energy capacity. They then propose the implementation of a blockchain network as a security layer for data sharing through IoT. This layer could mitigate IoT security issues with data encryption for transmitted data protection, user authentication through the blockchain network, and data decentralization. However, the authors note that the implementation of blockchain also brings challenges such as scalability, data transparency, transaction and processing speed, and low energy power of IoT equipment. The blockchain network itself could be an attack vector if not well implemented, such as 51 percent attacks (where the attacker takes control of 51 percent of the network nodes and can alter the validation of contracts) and violation of smart contracts by exploiting programming flaws. The challenges for implementation, as cited above, pass, according to the author, through the development and implementation of security factors in each of the layers. He suggests the implementation of security layers such as Explainable Artificial Intelligence (XAI) along with the blockchain, which evaluates and verifies data through the security standards that the AI was trained on. Finally, he suggests that the future should focus on the adaptability of the blockchain network to different scenarios and the development of blockchain systems explicitly adapted to IoT security. The main areas of focus include scalability, interoperability, energy efficiency, privacy preservation, and standardization.

The article (Zhang et al., 2020) discusses the use of Blockchain in the industry, particularly with IoT. Data from IoT devices may not be reliable, as many devices are not secure. It proposes the creation of a network called the Internet Blockchain of Things (IoT) to address the issue of trust in data from sensors. It also highlights the implementation challenges, especially scalability, and to solve these challenges, the multidisciplinary implementation of various concepts is suggested.

The article (Choi et al., 2021) addresses security issues in IoT devices for a specific case (Photovoltaic Panels). The authors point out vulnerabilities that can be exploited, such as lack of proper configuration, physical insecurity of the equipment, and weak user passwords. The article describes a type of attack called MITM, where the attacker can take on a role in the network, intercepting, capturing, or modifying data. The article then proposes a proof of concept where they set up a network with two edge devices acting as a blockchain to validate logins and data traffic between the photovoltaic panels and the server. They use Kali Linux to simulate an attacker and manage to validate the attack through the comparison of hashes between the IoT device and the server. Through blockchain, they can identify the attacking device and validate their proof of concept as positive.

The article (Márcio et al., 2021) discusses the concept of smart cities with devices connected to a large network and a significant number of IoT devices. It proposes the use of Smart Contracts and Blockchain as a security layer to validate the data produced by these devices. The article highlights that the main issues faced in an IoT network are: a lack of consensus among suppliers (different types of materials and protocols), access to devices, and updates for energy and firmware. The article suggests solving the security issues of IoT devices by validating data and authenticating their entry, creating a secure and decentralized network. It proposes a framework based on a blockchain network that integrates the physical layer (IoT sensors), communication, and the application interface. Using fog computing to validate the captured data and perform pre-processing, validating the data according to the smart contracts (reliable sources) before sending them to the higher cloud layer.

The article (Reilly et al., 2019) also addresses the application of IoT in smart cities. The authors especially highlight the problem of data integrity in IoT networks, and in the case of smart cities, this issue is severe because it can compromise critical cyber-physical systems. Among the problems mentioned are the lack of standardization in communication protocols, limited hardware resources, and varying device models. Such problems can be exploited by malicious actors and compromise the validity of the data trafficked. They propose the adoption of a blockchain as a layer to ensure data integrity. The authors analyze some existing IoT blockchains, highlighting the benefits and problems of adopting them (issues with scalability and vulnerability to 51 percent attacks are mentioned). They then propose a solution for data validation on a public network (to avoid the 51 percent attack) using Ethereum (as it is lightweight and can handle a significant volume of data). The created solution is tested on over 100 devices with satisfactory results, but with a transaction cost that could become high over time, given the high number of transactions.

The article (Cabrera-Gutiérrez et al., 2022) discusses the integration of Hardware Security Modules (HSM) and permissioned (private) blockchain in industrial IIoT networks. The article reports the growing adoption of IIoT devices for providing data for industrial intelligence, explains the increasing cyber threats, and proposes the adoption of a blockchain network as an advanced security layer. The authors then suggest the adoption of HSMs (for the protection of cryptographic access keys) integrated with a decentralized blockchain-based network. It details the integration of Hyperledger Fabric (blockchain) with TPM (HSM), focusing on critical operations like the enrollment of users and administrators, and the signing of transactions. It explains how these operations, traditionally performed by software tools, are executed internally in the TPM for greater security. The feasibility of this integration is discussed with a proof of concept implemented in an IoT node with a TPM2.0 HSM that interacts with a simulated Hyperledger Fabric blockchain network through a Raspberry Pi. Among the positive points, it highlights the security and integrity of data, reduced vulnerability, and decentralization. Among the negatives are the complexity of implementation, increased latency with the HSM, and scalability in a network with many devices.

The article (Garrocho et al., 2022) addresses the issue of communication failures in decentralized applications (DApps) that operate on IIoT devices, which interact with blockchain networks. It then discusses the failures that occur in DApps that are not addressed by consensus algorithms in message validation. The article identifies specific failures in communication between IIoT DApps and blockchain networks, such as network failures, submission failures, and response failures. It proposes methods to ”mask” these failures, allowing the DApps to continue functioning despite interruptions in communication with the blockchain network. It suggests modifications in smart contracts to avoid unnecessary processing and storage of repeated transactions resulting from the masking of failures. The evaluation of the failure model showed that it can increase the runtime for the creation and submission of transactions in the smart contract. The failure model provided greater resilience to the operations of DApps, which is essential for critical systems such as industrial systems, where failures can have serious consequences. However, it can also compromise the efficiency of the system, especially with larger transaction loads. The article suggests future improvements in the failure model, including the incorporation of other blockchain entities such as oracles, and plans to advance the evaluation of the model using an exponential distribution of failures.

In the article (Garrocho et al., 2023) the discussion revolves around the use of multi-robot systems in mining exploration and the challenges of creating and orchestrating software for robotics. It highlights the potential of blockchain to automate the sharing of maps through smart contracts in a traceable and auditable manner and proposes a Peer-to-Peer (P2P) blockchain network architecture embedded in robots. There is a section examining previous work related to mapping with robots and the security challenges in exchanging these maps, presenting blockchain as a crucial solution for making ad hoc communication between robots secure and decentralized. Another section focuses on edge computing and Edge Artificial Intelligence (Edge AI). The article then proposes the implementation of a multi-robot system with integrated blockchain. It details the system components, such as Simultaneous Localization and Mapping (SLAM), DApps for interaction with the blockchain, and the design of the architecture. The article then presents the implementation results, explains the component architecture, and discusses the evaluation results, highlighting poor performance in transaction confirmation as the map size increases and the challenges associated with implementing blockchain on embedded devices with limited resources. The authors conclude that the combination of blockchain and Edge AI in multi-robot systems offers significant benefits, such as tolerance to data loss, resistance to fraud, and reliable map exchange. However, they also acknowledge that there are challenges to be overcome, especially with respect to performance and energy consumption.

3 RESUME

Through the literature study of the 10 selected articles, we identified that the main problems reported with IIoT devices are: Data security and cyber vulnerabilities, data integrity and reliability, implementation and maintenance challenges, interoperability and standardization issues, energy consumption and limited resources, physical risks and human interference. Table 1 shows the number of citations to these problems.

Table 1: Challenges in IIoT.

Challenge in IIoT	Citations
Data Security and Cyber Vulnerabilities	3
Scalability and Efficiency	3
Data Integrity and Reliability	3
Maintenance Challenges	3
Interoperability	2
Energy Consumption	2
Physical Risks	2

Table 2 presents the main benefits of adopting blockchain in IIoT systems, as highlighted in the analyzed articles. The frequency of citations indicates the emphasis placed on each benefit in the related literature.

Table 2: Benefits of Blockchain in Industry 4.0.

Benefits of Adopting Blockchain in IIoT	Citations
Improvement in Data Security	4
Decentralization and Reliability	3
Data Immutability	2
Automation through Smart Contracts	2

4 OPEN ISSUES

The proposal to adopt blockchain in Industry 4.0 as a protective layer for data from IIoT devices, while promising, faces significant challenges. Table 3 addresses the main implementation challenges of this solution according to the authors.

Table 3: Challenges in Implementing Blockchain with IIoT.

Challenges	Citations
Scalability Challenges	3
Complexity of Implementation	3
Limited Resource	2
Risks Associated with Implementation	2
Interoperability Issues	1
Energy Efficiency	1
Maintenance Costs	1

5 ARCHITECTURE DESIGN

After conducting a thorough analysis of related work, we transitioned toward exploratory research through a proof of concept. Our primary objective in this phase was to investigate whether integrating a blockchain network could improve the security of data transmitted over an Industrial Internet of Things (IIoT) network, which was one of the problems highlighted in the related works. As shown in Figure 4, we propose developing a solution that enhances the reliability of the emitter by augmenting the data integrity features. To achieve this, we have created an architecture that verifies and validates data coming from a Programmable Logic Controller (PLC) using a blockchain network. Additionally, we utilize the Message Queuing Telemetry Transport (MQTT) protocol to transmit PLC data over the network since it has been widely used in the industry for communication between IIoT devices.

The PLC publishes data to an MQTT broker, and the blockchain network's nodes also connect to this broker. As a result, whenever the PLC sends (publishes) data to the broker, the blockchain nodes receive this data for validation. In the case of a legitimate device recognized by smart contracts, the data is stored in the blockchain. However, in the event of an unfavorable outcome, the system could generate a source inconsistency alert.

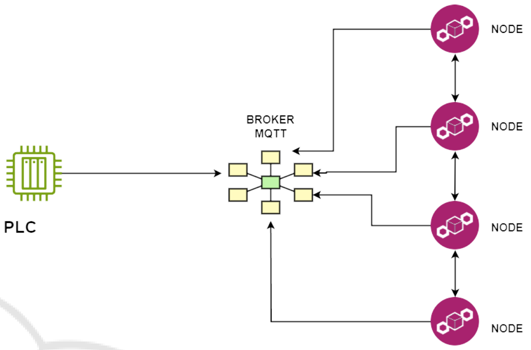


Figure 3: Architecture Design.

5.1 Node

We have created a blockchain network that aims to ensure that the data come from a legitimate source before recording it on the blockchain. In our scenario, the validation of the data-emitting device occurs through a smart contract executed on each node of the blockchain. This algorithm validates whether the device publishing on the broker's topic has a valid record on the blockchain. If it is valid, the published data is stored. In case of invalidity, we could generate an alert for data inconsistency and security incidents.

5.2 Proof of Concept – POC

In the initial phase, we subjected the data to a source validation algorithm, a preliminary step before storing it on the blockchain. This algorithm checks the authenticity of the data source. If the data come from a source validated by the blockchain, they are recorded. Otherwise, they are discarded, and a notification of inconsistency is issued.

For the tests, we used the PLC Nexto Xpress ALTUS 325, equipped with native support for the MQTT protocol. We implemented this protocol to initiate data transmission, acting as an MQTT publisher on the 'altus' topic. Along with the payload, we included a source validation key. Furthermore, we use a virtual machine configured with Raspberry Pi OS, serving as

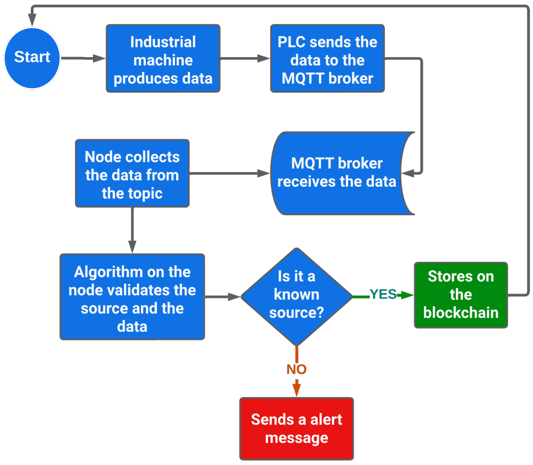

Start
Industrial machine produces data
PLC sends the data to the MQTT broker
MQTT broker receives the data
Node collects the data from the topic
Algorithm on the node validates the source and the data
Is it a known source?
YES
Stores on the blockchain
NO
Sends a alert message

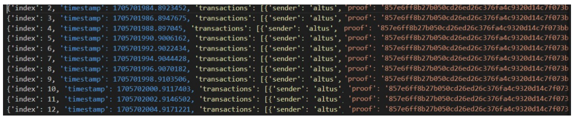
Figure 4: Logical sequence of the proof of concept.

an MQTT broker for message reception and distribution. This machine was configured with 2 1.8 GHz cores, 8GB of RAM, and 32 GB of storage. A second virtual machine, also with Raspberry Pi OS (2 cores at 1.8 GHz and 4 GB of RAM), was used for the validation and registration of messages on the blockchain. Additionally, we employed another device to simulate sending data from an unreliable or unknown source. The logical scheme with the data flow of the proof of concept is represented in a figure 4.

We conducted a POC focused on two fundamental functions: data validation and storage, aligned with the architecture we proposed. This study demonstrates how the integration of blockchain can add a layer of security, enhancing the integrity of data originating from industrial machines. This process ensures the reliable provenance of the data and the recording of all operations performed by the machine on the blockchain, thereby increasing the system's reliability.

We created an algorithm on the Altus PLC for data transmission using the MQTT protocol. In this algorithm, the publication topic, named 'altus', is first defined. The payload, which consists of the data to be sent, is carefully prepared. These data may include readings from analog and digital inputs. In this specific context, the data are appended with a hash value to ensure integrity. In addition, the algorithm specifies the size of the payload in bytes, a crucial piece of information for proper message processing. Finally, the algorithm determines whether the message should be retained ('stored') on the MQTT broker.

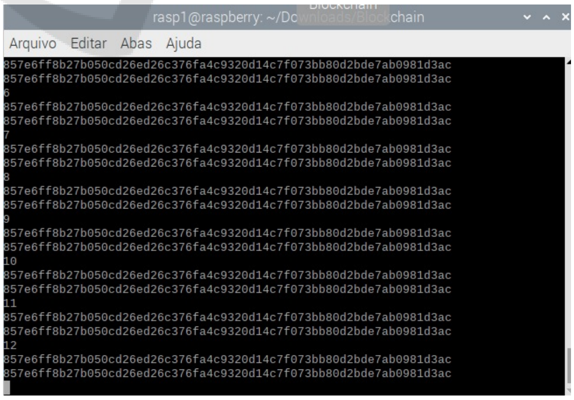
The MQTT broker was implemented using a Mosquitto server (Eclipse Mosquitto, 2023). This server is known for its lightweight and efficient handling of MQTT messages, making it the ideal choice for real-time data communication in industrial environments. The Mosquitto server facilitates the reception, processing, and distribution of messages published on the 'altus' topic. It manages multiple client connections, ensuring reliable message delivery and maintaining the integrity of the data flow. This includes the configuration of appropriate security measures, such as SSL/TLS encryption to protect data transmission and authentication protocols to prevent unauthorized access. This implementation was carried out on a virtual machine running the Raspberry Pi OS with network connectivity. The choice of Mosquitto for our implementation is due to its lightweight, open source, and extensive documentation and community support.



```
{'index': 2, 'timestamp': 1705701984.8923452, 'transactions': [{'sender': 'altus', 'proof': '857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073b
{'index': 3, 'timestamp': 1705701986.8947675, 'transactions': [{'sender': 'altus', 'proof': '857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073b
{'index': 4, 'timestamp': 1705701988.897045, 'transactions': [{'sender': 'altus', proof': '857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb
{'index': 5, 'timestamp': 1705701990.9006162, 'transactions': [{'sender': 'altus', 'proof': '857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073b
{'index': 6, 'timestamp': 1705701992.9022434, 'transactions': [{'sender': 'altus', 'proof': '857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073b
{'index': 7, 'timestamp': 1705701994.9044428, 'transactions': [{'sender': 'altus', 'proof': '857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073b
{'index': 8, 'timestamp': 1705701996.9070182, 'transactions': [{'sender': 'altus', 'proof': '857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073b
{'index': 9, 'timestamp': 1705701998.9103506, 'transactions': [{'sender': 'altus', 'proof': '857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073b
{'index': 10, 'timestamp': 1705702000.9117403, 'transactions': [{'sender': 'altus', 'proof': '857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073
{'index': 11, 'timestamp': 1705702002.9146502, 'transactions': [{'sender': 'altus', 'proof': '857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073
{'index': 12, 'timestamp': 1705702004.9171221, 'transactions': [{'sender': 'altus', 'proof': '857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073
```

Figure 5: Data block stored.

In our architecture, the blockchain node was set up on a virtual machine running Raspberry Pi OS, according to the specifications mentioned above. This machine serves as a blockchain node. During testing, we developed a Python solution that establishes a connection with the broker and receives data from the MQTT topic 'altus'. This solution is responsible for the validation of the data and its registration on the blockchain. After deploying this application on the virtual machine, we began the transmission and publication of data from the PLC. The data were successfully received by the node and stored in the corresponding block of our device, as illustrated in figure 5.

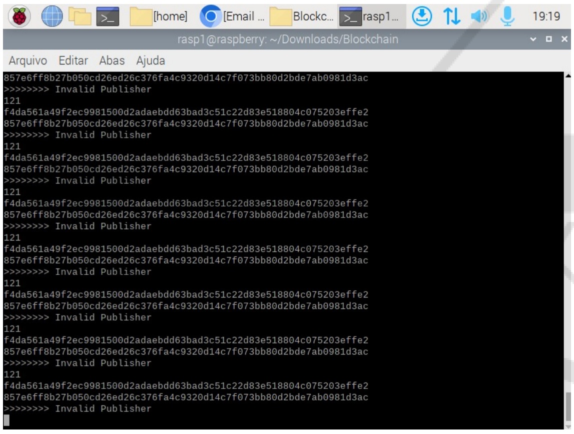


```
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
6
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
7
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
8
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
9
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
10
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
11
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
12
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
```

Figure 6: Valid Block with a hash valid.

To ensure data integrity, we compared the hashes already stored on the blockchain with a new hash generated from the data received from the topic (shown in Figure 6). If they match, the data is stored on the blockchain. Otherwise, it would indicate a potential source inconsistency, representing a possible security incident. In this scenario, the data is not stored and an inconsistency message is issued. The hash is generated using the cryptographic SHA-256 hash algorithm, an integral part of the Python Hashlib library. The preference for SHA-256 stems from its strong resistance to collision attacks, where two different data sets produce the same hash value, and its irreversible mapping feature, which makes it virtually impossible to deduce the original data from the generated hash value.

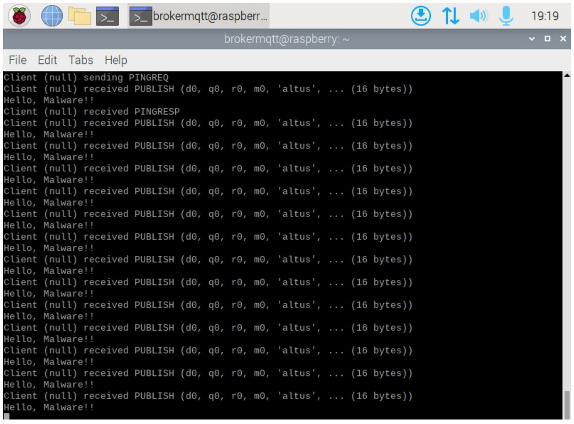
To test the integrity of the source, we published data from an unknown source (although MQTT provides security features in message publishing, such as login validation, we created an additional layer of security with blockchain) on the topic ”altus”. The generated hash is different from those that already exist and have been stored; therefore, the block is discarded, and a data inconsistency message is generated (shown in Figure 7).



```
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
>>>>>>>> Invalid Publisher
121
f4da561a49f2ec9981500d2adaebdd63bad3c51c22d83e518804c075203effe2
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
>>>>>>>> Invalid Publisher
121
f4da561a49f2ec9981500d2adaebdd63bad3c51c22d83e518804c075203effe2
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
>>>>>>>> Invalid Publisher
121
f4da561a49f2ec9981500d2adaebdd63bad3c51c22d83e518804c075203effe2
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
>>>>>>>> Invalid Publisher
121
f4da561a49f2ec9981500d2adaebdd63bad3c51c22d83e518804c075203effe2
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
>>>>>>>> Invalid Publisher
121
f4da561a49f2ec9981500d2adaebdd63bad3c51c22d83e518804c075203effe2
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
>>>>>>>> Invalid Publisher
121
f4da561a49f2ec9981500d2adaebdd63bad3c51c22d83e518804c075203effe2
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
>>>>>>>> Invalid Publisher
121
f4da561a49f2ec9981500d2adaebdd63bad3c51c22d83e518804c075203effe2
857e6ff8b27b050cd26ed26c376fa4c9320d14c7f073bb80d2bde7ab0981d3ac
>>>>>>>> Invalid Publisher
```

Figure 7: Invalid Block with an alert message.

Furthermore, we conducted a simulation to understand the implications of potential unauthorized access by malicious agents to the MQTT broker for publishing. We observed that, in the absence of a hash validation algorithm on the blockchain, devices subscribed to the ’altus’ topic could be vulnerable to unwanted exposures. To illustrate this risk, we intentionally sent the message ’Hello, Malware’ through the system (shown in Figure 8). This message was effectively received by the subscriber(without the algorithm) of the topic, demonstrating how potentially malicious data could be consumed in a real-world scenario. This experiment highlights the importance of robust security mechanisms to prevent cybersecurity incidents in systems that depend on the integrity and reliability of data communication.



```
Client (null) sending PINGREQ
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
Client (null) received PINGRESP
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
Client (null) received PUBLISH (d0, q0, r0, m0, 'altus', ... (16 bytes))
Hello, Malware!!
```

Figure 8: Exposure to a topic with data from a malicious source.

5.3 Study Limitations

In our implementation, we focus on the aspects of data source validation for recording on the blockchain through the MQTT protocol. In this study, we did not delve into the security aspects of MQTT and the Eclipse Mosquitto server, although they have robust native security features. The implementation also used virtualized resources for testing (MQTT broker and blockchain node), while the ALTUS PLC is physical. The proposed solution was carried out in a controlled environment, where it was successful, but requires more robust security and performance tests to validate the implementation and place it in a real environment, which will be carried out in future works.

6 FINAL CONSIDERATIONS

Cyber-physical device attacks have intensified since Stuxnet, and we propose the adoption of blockchain as a protective layer for data integrity shared through IIoT devices. This study, through a review of the literature, highlights the deficiencies of IIoT technologies, especially in terms of data integrity, and how blockchain can serve as a mitigating factor for cyber vulnerabilities in this scenario. The study also shows that, although promising, adoption is not simple and presents challenges, particularly in solution scalability and integration with limited-resource equipment.

Our case study demonstrated the feasibility of transmitting data from industrial machines to the blockchain via MQTT, a lightweight and secure protocol. We observed positive results, indicating the potential of blockchain for secure and integral communications in industrial environments. In future work, we will deepen the investigation of this solution in more complex scenarios.

6.1 Future Work

In future works, our aim is to expand the concepts presented in this article into a real-world setting, implementing an entire network with physical devices. Our goal is to test the resilience of this architecture against cyber threats such as MitM DoS attacks. In addition, we will explore the scalability of the system under different loads in specific industrial scenarios, including a detailed analysis of network performance and data integrity in real operational conditions. We also plan to investigate the integration of advanced techniques in blockchain usage to enhance the system's security and efficiency. This comprehensive approach will provide deeper insights into the practical application and robustness of our proposed solution in industrial IoT environments.

REFERENCES

Akshatha, P. and Dilip Kumar, S. (2023). Mqtt and blockchain sharding: An approach to user-controlled data access with improved security and efficiency. *Blockchain: Research and Applications*, 4(4):100158.

Alajlan, R., Alhumam, N., and Frikha, M. (2023). Cybersecurity for blockchain-based iot systems: A review. *Applied Sciences*, 13(13).

Angle, M. G., Madnick, S., Kirtley, J. L., and Khan, S. (2019). Identifying and anticipating cyberattacks that could cause physical damage to industrial control systems. *IEEE Power and Energy Technology Systems Journal*, 6(4):172–182.

Cabrera-Gutiérrez, A. J., Castillo, E., Escobar-Molero, A., Álvarez Bermejo, J. A., Morales, D. P., and Parrilla, L. (2022). Integration of hardware security modules and permissioned blockchain in industrial iot networks. *IEEE Access*, 10:114331–114345.

Choi, J., Ahn, B., Bere, G., Ahmad, S., Mantooth, H. A., and Kim, T. (2021). Blockchain-based man-in-the-middle (mitm) attack detection for photovoltaic systems. In *2021 IEEE Design Methodologies Conference (DMC)*, pages 1–6.

Eclipse Mosquitto (2023). An open source mqtt broker. http://www.mosquitto.org. [Online; accessed 20-Nov-2023].

Fernández-Caramés, T. M. and Fraga-Lamas, P. (2019). A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. *IEEE Access*, 7:45201–45218.

Garrocho, C. T., de Sousa, F. L., Silva, M. C., and Oliveira, R. A. (2023). Blockchain-based smart contract and edge ai applied in a multirobot system: An approach. *IEEE Robotics & Automation Magazine*, pages 2–10.

Garrocho, C. T. B., Oliveira, K. N., Santos, A. L. d., da Cunha Cavalcanti, C. F. M., and Oliveira, R. A. R. (2022). Toward a failures model for communication of decentralized applications with blockchain networks applied in the industrial environment. *IEEE Wireless Communications*, 29(3):40–46.

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele Univ.*, 33.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3):49–51.

Márcio, C., Ferreira, C. M., Tim, C., Garrocho, B., Augusto, R., Rabelo, R., Sá Silva, J., Frederico, C., Da, M., and Cavalcanti, C. (2021). Iot registration and authentication in smart city applications with blockchain. *Sensors*, 21.

Reilly, E., Maloney, M., Siegel, M., and Falco, G. (2019). An iot integrity-first communication protocol via an ethereum blockchain light client. In *2019 IEEE/ACM 1st International Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT)*, pages 53–56.

Zhang, Z., Huang, L., Tang, R., Peng, T., Guo, L., and Xiang, X. (2020). Industrial blockchain of things: A solution for trustless industrial data sharing and beyond. In *2020 IEEE 16th International Conference on Automation Science and Engineering (CASE)*, pages 1187–1192.